IN THE CLAIMS:

1-35. (cancelled)

36. (renumbered 32) (currently amended) A method to protect from unauthorized access an electronic data object created to store information, comprising the steps of:

providing a separate user storage for association of user identifiers dependent on previously determined user ID information;

providing a separate data object category storage for association of data object identifiers and access right categories, said data object identifiers forming structural connections to types of people or contextual associations with subject areas, and said data object identifiers also reflecting structural connections to studies or findings;

providing a separate access right storage for association of said user identifiers with said access ~~read~~ <u>right</u> categories;

determining an access right dependent on the data object identifier and also on the user identifier by use of said user storage and said data object category storage, and when determining said access right, also determining an association of the user identifier with at least one of the access right categories so that the access right is also dependent on the association of the user identifier with the at least one access right category; and

allowing the access by operating personnel to the data object dependent on the access right.

37. (renumbered 33) (previously presented) A method to protect from unauthorized access an electronic data object created to store information, comprising the steps of:

providing a separate user storage for association of user identifiers dependent on previously determined user ID information;

providing a separate data object category storage for association of data object identifiers and access right categories, said data object identifiers forming structural connections comprising at least one of work groups, research teams, personnel hierarchies, contents referring to people, or contextual associations with subject areas or studies in systems of the access rights, and said data object identifiers also reflecting at least one of affiliation with clinical studies, with series of diagnostic findings, or exposures over a long period of time, or with specific diagnostic image types;

providing a separate access right storage for association of said user identifiers with said access right categories;

determining an access right dependent on the data object identifier and also on the user identifier by use of said user storage and said data object category storage, and when determining said access right, also determining an association of the user identifier with at least one of the access right categories, so that by use of said access right storage the access right is also determined dependent on the association of the user identifier with the at least one access right category; and

along the access by the operating personnel to the data object dependent on the access right.